KTH Computer Science
and Communication

Proof of Work

An evaluation of proof of work as a DOS prevention method

FREDRIK LILKAER, CHRISTOPHER TELJSTEDT

Bachelor's Thesis
Supervisor: Douglas Wikström

Chapter 1

Introduction

1.1 Background

One of the most significant threats in server security are Denial of Service (DoS) attacks. It is essentially a targeted effort to prevent a service from functioning properly by draining the underlying computer resources. There are different levels of the attacks which either can be targeted to exploit vulnerabilities in the TCP/IP-protocol, in the operation system that the server runs on or more specific implementations of the service. [källa på det här]

Recently, researchers have shown an increased interest in the Proof of Work (PoW) concept in order to prevent or mitigate the effects of a DoS attack on such systems. The idea is to require the clients to solve an instance of a predefined problem in order to gain access to the server's resources. To cope with a potential DoS attacks the level of difficulty of the problems is scaled proportionally with the amount stress that is put on the system. [källa på det här]

1.2 Problem definition

The global difficulty could potentially work as a prevention mechanism to at least mitigate the effects of a DoS attack without making an as assumption about the source. However, this is also what brings the current implementations of Proof of Work to it's knees. The classical implementation of Proof of Work does not seperate legitimate users from attackers. Hence, a Proof of Work protected system under stress would also send hard problems to legitimate users resulting in long response times. This also affects users that access the system with devices equipped weaker hardware in terms of performance, i.e. mobile devices and computers with out of date hardware, which then would require more effort to solve the problems.

1.3 Problem statement

With the problem defined the question at hand is thus if it is possible to develop a Proof of Work protocol that is independent of client characteristics.

- Is there a viable way to implement a Proof of Work system so that the system's resources are accessable by a diverse variety of devices?
- How should the protocol be optimised for low impact on legitimate client behaviour and high impact on malicious behaviour?
- What advantages and disadvantages does proof of work concept bring in practice and in which applications could it be an improvement to current security?

Chapter 2

Purpose and method

The purpose of this study is to research ways to improve the classical Proof of Work in such a way that legitimate users are less affected by the Proof of Work than the participants of a DoS attack. Furthermore find a way to dynamically scale the required proof of work when dealing with different hardware.

2.1 Scope and delimitations

Scope:
The coverage of this study .....
The study consists of .....
The study covers the .....
This study is focus on .....

Delimitations:
The study does not cover the .....
The researcher limited this research to .....
This study is limited to .....

2.2 Methodology

Chapter 3

Theoretical perspective